

# National Cyber Alert System

## Cyber Security Bulletin SB09-138

[Archive](#)

### Vulnerability Summary for the Week of May 11, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source
.t-dreams -- job_career_package	Techno Dreams Job Career Package 3.0 allows remote attackers to bypass authentication and obtain administrative access by setting the JobCareerAdmin cookie to Login.	2009-05-15	7.5	CVE-1638 XF BID MLA SECU OSVI
apple -- safari	Apple Safari executes DOM calls in response to a javascript: URI in the target attribute of a submit element within a form contained in an inline PDF file, which might allow remote attackers to bypass intended Adobe Acrobat JavaScript restrictions on accessing the document object, as demonstrated by a web site that permits PDF uploads by untrusted users, and therefore has a shared document.domain between the web site and this javascript: URI. NOTE: the researcher reports that Adobe's position is "a PDF file is active content."	2009-05-11	9.3	CVE-1600 BUG MISC
apple -- mac_os_x	The kernel in Apple Mac OS X 10.5 before 10.5.7 does not properly check indexes during the handling of workqueues, which	2009-05-	7.0	CVE-1517

apple -- mac_os_x_server	allows local users to gain privileges or cause a denial of service (system shutdown) via unspecified vectors.	13	7.2	CON: APPI
apple -- mac_os_x	Integer underflow in QuickDraw Manager in Apple Mac OS X 10.4.11 and 10.5 before 10.5.7 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted PICT image that triggers a heap-based buffer overflow.	2009-05-13	9.3	CVE-0010 CON: APPI
apple -- mac_os_x apple -- mac_os_x_server	Apple Mac OS X 10.4.11 and 10.5 before 10.5.7 allows local users to gain privileges or cause a denial of service (application crash) by attempting to mount a crafted sparse disk image that triggers memory corruption.	2009-05-13	7.5	CVE-0149 CON: APPI
apple -- safari	WebKit, as used in Safari before 3.2.3 and 4 Public Beta, on Apple Mac OS X 10.4.11 and 10.5 before 10.5.7 and Windows allows remote attackers to execute arbitrary code via a crafted SVGList object that triggers memory corruption.	2009-05-13	9.3	CVE-0945 CON: APPI APPI APPI
baofeng -- storm	Stack-based buffer overflow in the MPS.StormPlayer.1 ActiveX control in mps.dll 3.9.4.27 in Baofeng Storm allows remote attackers to execute arbitrary code via a long argument to the OnBeforeVideoDownload method. NOTE: some of these details are obtained from third party information.	2009-05-11	9.3	CVE-1612 BID
carnegie_mellon_university -- cyrus-sasl	Multiple buffer overflows in the CMU Cyrus SASL library before 2.1.23 might allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via strings that are used as input to the sasl_encode64 function in lib/saslutil.c.	2009-05-15	7.5	CVE-0688 CERT BID CON:
cisco -- wvc54gc	The Cisco Linksys WVC54GCA wireless video camera with firmware 1.00R22 and 1.00R24 stores passwords and wireless-network keys in cleartext in (1) pass_wd.htm and (2) Wsecurity.htm, which allows remote attackers to obtain sensitive information by reading the HTML source code.	2009-05-06	7.8	CVE-1560 XF VUPI MISC
cscope -- cscope	Multiple buffer overflows in Cscope before 15.7a allow remote attackers to execute arbitrary code via long strings in input such as (1) source-code tokens and (2) pathnames, related to integer overflows in some cases. NOTE: this issue exists because of an incomplete fix for CVE-2004-2541.	2009-05-05	9.3	CVE-0148 CON: CON:
cscope -- cscope	Multiple stack-based buffer overflows in the putstring function in find.c in Cscope before 15.6 allow user-assisted remote attackers to execute arbitrary code via a long (1) function name or (2) symbol in a source-code file.	2009-05-07	9.3	CVE-1577 CON: CON: CON:
	Multiple stack-based and heap-based buffer overflows in Dafolo DafoloControl ActiveX control (DafoloFFControl.dll) 1.108.6.195 allow remote attackers to execute arbitrary			CVE-1606 XF

dafolo -- dafolocontrol	code via long (1) baseurl, (2) kommune, (3) felter, (4) afdeling, (5) Flags, (6) HelpURL, (7) caburl, or (8) filename properties; or (9) a long argument to the Open method. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-05-11	9.3	XF XF XF BID SECU
ecshop -- ecshop	SQL injection vulnerability in user.php in EcShop 2.5.0 allows remote attackers to execute arbitrary SQL commands via the order_sn parameter in an order_query action.	2009-05-12	7.5	CVE-1622 BID MILV
electrasoft -- 32bit_ftp	Stack-based buffer overflow in ElectraSoft 32bit FTP 09.04.24 allows remote FTP servers to execute arbitrary code via a long banner. NOTE: this might overlap CVE-2003-1368.	2009-05-08	10.0	CVE-1592 BID MILV MILV
electrasoft -- 32bit_ftp	Stack-based buffer overflow in ElectraSoft 32bit FTP 09.04.24 allows remote FTP servers to execute arbitrary code via a long 257 reply to a CWD command.	2009-05-11	10.0	CVE-1611 BID MILV
garmin -- garmin_communicator_plugin	The domain-locking implementation in the GARMINAXCONTROL.GarminAxControl_t.1 ActiveX control in npGarmin.dll in the Garmin Communicator Plug-In 2.6.4.0 does not properly enforce the restrictions that (1) download and (2) upload requests come from a web site specified by the user, which allows remote attackers to obtain sensitive information or reconfigure Garmin GPS devices via unspecified vectors related to a "synchronisation error."	2009-05-11	9.3	CVE-0194 XF BID BUG SECT MISC SECU OSVI
google -- chrome	Heap-based buffer overflow in the ParamTraits::Read function in Google Chrome before 1.0.154.64 allows attackers to leverage renderer access to cause a denial of service (application crash) or possibly execute arbitrary code via vectors related to a large bitmap that arrives over the IPC channel.	2009-05-07	9.3	CVE-1441 CON CON
google -- chrome	Google Chrome executes DOM calls in response to a javascript: URI in the target attribute of a submit element within a form contained in an inline PDF file, which might allow remote attackers to bypass intended Adobe Acrobat JavaScript restrictions on accessing the document object, as demonstrated by a web site that permits PDF uploads by untrusted users, and therefore has a shared document.domain between the web site and this javascript: URI. NOTE: the researcher reports that Adobe's position is "a PDF file is active content."	2009-05-11	9.3	CVE-1598 BUG MISC
hp -- openview_network_node_manager	Unspecified vulnerability in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to execute arbitrary code via unknown vectors.	2009-05-05	10.0	CVE-0720 HP HP

hp -- data_protector_express	Unspecified vulnerability in HP Data Protector Express and Express SSE 3.x before build 47065, and Express and Express SSE 4.x before build 46537, allows local users to gain privileges or cause a denial of service via unknown vectors.	2009-05-14	7.2	CVE-0714 SECU HP HP
ibiblio -- osprey	PHP remote file inclusion vulnerability in ListRecords.php in osprey 1.0a4.1 allows remote attackers to execute arbitrary PHP code via a URL in the xml_dir parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. NOTE: the lib_dir vector is already covered by CVE-2006-6630.	2009-05-12	7.5	CVE-6807 XF BID
ibm -- tivoli_storage_manager_client ibm -- tivoli_storage_manager_express	Multiple stack-based buffer overflows in dsmagent.exe in the Remote Agent Service in the IBM Tivoli Storage Manager (TSM) client 5.1.0.0 through 5.1.8.2, 5.2.0.0 through 5.2.5.3, 5.3.0.0 through 5.3.6.4, and 5.4.0.0 through 5.4.1.96, and the TSM Express client 5.3.3.0 through 5.3.6.4, allow remote attackers to execute arbitrary code via (1) a request packet that is not properly parsed by an unspecified "generic string handling function" or (2) a crafted nodeName in a dicuGetIdentifyRequest request packet, related to the (a) Web GUI and (b) Java GUI.	2009-05-05	10.0	CVE-4828 AIXA CON.
ibm -- tivoli_storage_manager_client ibm -- tivoli_storage_manager_express	Buffer overflow in the Web GUI in the IBM Tivoli Storage Manager (TSM) client 5.1.0.0 through 5.1.8.2, 5.2.0.0 through 5.2.5.3, 5.3.0.0 through 5.3.6.4, 5.4.0.0 through 5.4.2.6, and 5.5.0.0 through 5.5.1.17 allows attackers to cause a denial of service (application crash) or execute arbitrary code via unspecified vectors.	2009-05-05	10.0	CVE-1520 XF VUPI AIXA CON. SECU
ibm -- tivoli_storage_manager_client ibm -- tivoli_storage_manager_express	Unspecified vulnerability in the Java GUI in the IBM Tivoli Storage Manager (TSM) client 5.2.0.0 through 5.2.5.3, 5.3.0.0 through 5.3.6.5, 5.4.0.0 through 5.4.2.6, and 5.5.0.0 through 5.5.1.17, and the TSM Express client 5.3.3.0 through 5.3.6.5, allows attackers to read or modify arbitrary files via unknown vectors.	2009-05-05	7.5	CVE-1521 AIXA CON.
ibm -- tivoli_storage_manager_client	The IBM Tivoli Storage Manager (TSM) client 5.5.0.0 through 5.5.1.17 on AIX and Windows, when SSL is used, allows remote attackers to conduct unspecified man-in-the-middle attacks and read arbitrary files via unknown vectors.	2009-05-05	7.1	CVE-1522 AIXA CON.
jobscript -- job_script_job_board_software	admin/changepassword.php in Job Script Job Board Software 2.0 allows remote attackers to change the administrator password and gain administrator privileges via a direct request.	2009-05-11	7.5	CVE-1610 XF BID MILV SECU OSVI

klinzmann -- application_access_server	Application Access Server (A-A-S) 2.0.48 has "wildbat" as its default password for the admin account, which makes it easier for remote attackers to obtain access.	2009-05-14	7.5	CVE-1465 MISC BID BUG SECT
kowalczyk -- sumatrapdf	Heap-based buffer overflow in the loadexponentialfunc function in mupdf/pdf_function.c in MuPDF in the mupdf-20090223-win32 package, as used in SumatraPDF 0.9.3 and earlier, allows remote attackers to execute arbitrary code via a crafted PDF file. NOTE: some of these details are obtained from third party information.	2009-05-11	9.3	CVE-1605 VUPI VUPI SECU FULI
limesurvey -- limesurvey	Unspecified vulnerability in LimeSurvey before 1.82 allows remote attackers to execute commands and obtain sensitive data via unknown attack vectors related to /admin/remotecontrol/.	2009-05-11	7.5	CVE-1604 VUPI CON
mcafee -- groupshield	McAfee GroupShield for Microsoft Exchange on Exchange Server 2000, and possibly other anti-virus or anti-spam products from McAfee or other vendors, does not scan X-headers for malicious content, which allows remote attackers to bypass virus detection via a crafted message, as demonstrated by a message with an X-Testing header and no message body.	2009-05-05	10.0	CVE-1491 XF MISC
microchip -- mplab_ide	Multiple buffer overflows in Microchip MPLAB IDE 8.30 and possibly earlier versions allow user-assisted remote attackers to execute arbitrary code via a .MCP project file with long (1) FILE_INFO, (2) CAT_FILTERS, and possibly other fields.	2009-05-11	9.3	CVE-1608 BID BUG MISC SECU
microsoft -- office_powerpoint	Multiple stack-based buffer overflows in the PowerPoint 4.0 importer (PP4X32.DLL) in Microsoft Office PowerPoint 2000 SP3, 2002 SP3, and 2003 SP3 allow remote attackers to execute arbitrary code via crafted formatting data for paragraphs in a file that uses a PowerPoint 4.0 native file format, related to (1) an incorrect calculation from a record header, or (2) an interget that is used to specify the number of bytes to copy, aka "Legacy File Format Vulnerability."	2009-05-12	9.3	CVE-0220 CERT
microsoft -- office_powerpoint	Integer overflow in Microsoft Office PowerPoint 2002 SP3 and 2003 SP3 allows remote attackers to execute arbitrary code via an invalid record type in a PowerPoint file that triggers memory corruption, aka "Integer Overflow Vulnerability."	2009-05-12	9.3	CVE-0221 CERT
microsoft -- office_powerpoint	Microsoft Office PowerPoint 2000 SP3, 2002 SP3, and 2003 SP3 allows remote attackers to execute arbitrary code via crafted sound data in a file that uses a PowerPoint 4.0 native file format, leading to a "pointer overwrite" and memory corruption, aka	2009-05-12	9.3	CVE-0222 CERT

	"Legacy File Format Vulnerability," a different vulnerability than CVE-2009-0223, CVE-2009-0226, CVE-2009-0227, and CVE-2009-1137.			<a href="#">CVE-2009-0223</a>
microsoft -- office_powerpoint	Microsoft Office PowerPoint 2000 SP3, 2002 SP3, and 2003 SP3 allows remote attackers to execute arbitrary code via crafted sound data in a file that uses a PowerPoint 4.0 native file format, leading to memory corruption, aka "Legacy File Format Vulnerability," a different vulnerability than CVE-2009-0222, CVE-2009-0226, CVE-2009-0227, and CVE-2009-1137.	2009-05-12	9.3	<a href="#">CVE-0223</a> <a href="#">CERT</a>
microsoft -- compatibility_pack_word_excel_powerpoint microsoft -- office_compatibility_pack_for_word_excel_ppt_2007 microsoft -- office_powerpoint microsoft -- office_powerpoint_viewer microsoft -- open_xml_file_format_converter microsoft -- powerpoint microsoft -- works	Microsoft Office PowerPoint 2000 SP3, 2002 SP3, 2003 SP3, and 2007 SP1 and SP2; PowerPoint Viewer 2003 and 2007 SP1 and SP2; PowerPoint in Microsoft Office 2004 for Mac and 2008 for Mac; Open XML File Format Converter for Mac; Microsoft Works 8.5 and 9.0; and Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2 do not properly validate list records in PowerPoint files, which allows remote attackers to execute arbitrary code via a crafted file that triggers memory corruption related to an invalid record type, aka "Memory Corruption Vulnerability."	2009-05-12	9.3	<a href="#">CVE-0224</a> <a href="#">CERT</a>
microsoft -- office_powerpoint	Microsoft Office PowerPoint 2002 SP3 allows remote attackers to execute arbitrary code via crafted sound data in a file that uses a PowerPoint 95 native file format, leading to improper "array indexing" and memory corruption, aka "PP7 Memory Corruption Vulnerability."	2009-05-12	9.3	<a href="#">CVE-0225</a> <a href="#">CERT</a>
microsoft -- office_powerpoint	Stack-based buffer overflow in the PowerPoint 4.2 conversion filter in Microsoft Office PowerPoint 2000 SP3, 2002 SP3, and 2003 SP3 allows remote attackers to execute arbitrary code via a long string in sound data in a file that uses a PowerPoint 4.0 native file format, leading to memory corruption, aka "Legacy File Format Vulnerability," a different vulnerability than CVE-2009-0222, CVE-2009-0223, CVE-2009-0227, and CVE-2009-1137.	2009-05-12	9.3	<a href="#">CVE-0226</a> <a href="#">CERT</a>
microsoft -- office_powerpoint	Stack-based buffer overflow in the PowerPoint 4.2 conversion filter (PP4X32.DLL) in Microsoft Office PowerPoint 2000 SP3, 2002 SP3, and 2003 SP3 allows remote attackers to execute arbitrary code via a large number of structures in sound data in a file that uses a PowerPoint 4.0 native file format, leading to memory corruption, aka "Legacy File Format Vulnerability," a different vulnerability than CVE-2009-0222, CVE-2009-0223, CVE-2009-0226, and CVE-2009-1137.	2009-05-12	9.3	<a href="#">CVE-0227</a> <a href="#">CERT</a>

microsoft -- office_powerpoint	Microsoft Office PowerPoint 2000 SP3, 2002 SP3, and 2003 SP3 allows remote attackers to execute arbitrary code via crafted sound data in a file that uses a PowerPoint 95 native file format, leading to memory corruption, aka "PP7 Memory Corruption Vulnerability," a different vulnerability than CVE-2009-1129.	2009-05-12	9.3	CVE-1128 CERT
microsoft -- office_powerpoint	Multiple stack-based buffer overflows in the PowerPoint 95 importer (PP7X32.DLL) in Microsoft Office PowerPoint 2000 SP3, 2002 SP3, and 2003 SP3 allow remote attackers to execute arbitrary code via an inconsistent record length in sound data in a file that uses a PowerPoint 95 (PPT95) native file format, aka "PP7 Memory Corruption Vulnerability," a different vulnerability than CVE-2009-1128.	2009-05-12	9.3	CVE-1129 CERT
microsoft -- office microsoft -- office_powerpoint	Heap-based buffer overflow in Microsoft Office PowerPoint 2002 SP3 and 2003 SP3, and PowerPoint in Microsoft Office 2004 for Mac, allows remote attackers to execute arbitrary code via a crafted structure in a Notes container in a PowerPoint file that causes PowerPoint to read more data than was allocated when creating a C++ object, leading to an overwrite of a function pointer, aka "Heap Corruption Vulnerability."	2009-05-12	9.3	CVE-1130 CERT MISC VUPI SECT BID BUG MS SECU
microsoft -- office_powerpoint	Multiple stack-based buffer overflows in Microsoft Office PowerPoint 2000 SP3 allow remote attackers to execute arbitrary code via a large amount of data associated with unspecified atoms in a PowerPoint file that triggers memory corruption, aka "Data Out of Bounds Vulnerability."	2009-05-12	10.0	CVE-1131 CERT VUPI SECT BID BUG MS MISC SECU
microsoft -- office_powerpoint	Microsoft Office PowerPoint 2000 SP3, 2002 SP3, and 2003 SP3 allows remote attackers to execute arbitrary code via crafted sound data in a file that uses a PowerPoint 4.0 native file format, leading to memory corruption, aka "Legacy File Format Vulnerability," a different vulnerability than CVE-2009-0222, CVE-2009-0223, CVE-2009-0226, and CVE-2009-0227.	2009-05-12	9.4	CVE-1137 CERT XF VUPI SECT BID MS SECU
mini-stream -- mini-stream_rm_downloader	Multiple stack-based buffer overflows in Mini-stream Ripper 3.0.1.1 allow remote attackers to execute arbitrary code via (1) a long rtsp URL in a .ram file and (2) a long string in the HREF attribute of a REF element in a .asx file.	2009-05-15	9.3	CVE-1641 XF BID BID MILV MILV
mini-stream -- mini-stream_to_mp3_converter	Multiple stack-based buffer overflows in Mini-stream ASX to MP3 Converter 3.0.0.7 allow remote attackers to execute arbitrary code via (1) a long rtsp URL in a .ram file	2009-05-15	9.3	CVE-1642 XF BID BID

	and (2) a long string in the HREF attribute of a REF element in a .asx file.			<a href="#">DID</a> <a href="#">MILV</a> <a href="#">MILV</a>
mini-stream -- easy_rm-mp3_converter	Multiple stack-based buffer overflows in Mini-stream Easy RM-MP3 Converter 3.0.0.7 allow remote attackers to execute arbitrary code via (1) a long rtsp URL in a .ram file and (2) a long string in the HREF attribute of a REF element in a .asx file.	2009-05-15	9.3	<a href="#">CVE-1645</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">BID</a> <a href="#">MILV</a> <a href="#">MILV</a>
mini-stream -- mini-stream_rm_downloader	Stack-based buffer overflow in Mini-stream RM Downloader 3.0.0.9 allows remote attackers to execute arbitrary code via a long rtsp URL in a .ram file.	2009-05-15	9.3	<a href="#">CVE-1646</a> <a href="#">BID</a> <a href="#">MILV</a>
mozilla -- firefox	Mozilla Firefox executes DOM calls in response to a javascript: URI in the target attribute of a submit element within a form contained in an inline PDF file, which might allow remote attackers to bypass intended Adobe Acrobat JavaScript restrictions on accessing the document object, as demonstrated by a web site that permits PDF uploads by untrusted users, and therefore has a shared document.domain between the web site and this javascript: URI. NOTE: the researcher reports that Adobe's position is "a PDF file is active content."	2009-05-11	9.3	<a href="#">CVE-1597</a> <a href="#">BUG</a> <a href="#">MISC</a>
nucleustechnologies -- kernel_recovery	Stack-based buffer overflow in Nucleus Data Recovery Kernel Recovery for Macintosh 4.04 allows user-assisted attackers to execute arbitrary code via a crafted .AMHH file.	2009-05-15	9.3	<a href="#">CVE-1640</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">SECU</a> <a href="#">OSVI</a>
opera -- opera_browser	Opera executes DOM calls in response to a javascript: URI in the target attribute of a submit element within a form contained in an inline PDF file, which might allow remote attackers to bypass intended Adobe Acrobat JavaScript restrictions on accessing the document object, as demonstrated by a web site that permits PDF uploads by untrusted users, and therefore has a shared document.domain between the web site and this javascript: URI. NOTE: the researcher reports that Adobe's position is "a PDF file is active content."	2009-05-11	9.3	<a href="#">CVE-1599</a> <a href="#">BUG</a> <a href="#">MISC</a>
qsix -- blusky_cms	SQL injection vulnerability in index.php in BluSky CMS allows remote attackers to execute arbitrary SQL commands via the news_id parameter in a read action.	2009-05-06	7.5	<a href="#">CVE-1548</a> <a href="#">VUPI</a> <a href="#">MILV</a> <a href="#">SECU</a> <a href="#">OSVI</a>
qt-cute -- quickteam	Multiple PHP remote file inclusion vulnerabilities in Qt quickteam 2 allow remote attackers to execute arbitrary PHP code via a URL in the (1) qte_web_path	2009-05-06	7.5	<a href="#">CVE-1551</a> <a href="#">VUPI</a> <a href="#">MILV</a> <a href="#">SECU</a>

	parameter to qte_web.php and the (2) qte_root parameter to bin/qte_init.php.			SEC OSVI OSVI
scripts-for-sites -- ez_link_directory	SQL injection vulnerability in links.php in Scripts for Sites (SFS) EZ Link Directory allows remote attackers to execute arbitrary SQL commands via the cat_id parameter in a list action.	2009-05-12	7.5	CVE-6808 BID MILV
sdp_multimedia -- streaming_download_project	Stack-based buffer overflow in Streaming Download Project (SDP) Downloader 2.3.0 allows remote attackers to execute arbitrary code via a long .asf URL in the HREF attribute of a REF element in a .asx file.	2009-05-12	9.3	CVE-1627 VUPI BID MILV MILV SECU OSVI
sorinara -- soritong_mp3_player	Stack-based buffer overflow in Sorinara Soritong MP3 Player 1.0 allows remote attackers to execute arbitrary code via a crafted .m3u file.	2009-05-15	9.3	CVE-1643 XF BID MILV
sorinara -- streaming_audio_player	Stack-based buffer overflow in Sorinara Streaming Audio Player 0.9 allows remote attackers to execute arbitrary code via a crafted .pla file.	2009-05-15	9.3	CVE-1644 XF BID MILV MILV
squirrelmail -- squirrelmail	Session fixation vulnerability in SquirrelMail before 1.4.18 allows remote attackers to hijack web sessions via a crafted cookie.	2009-05-14	7.6	CVE-1580 VUPI CON CON
teraway -- linktracker	Teraway LinkTracker 1.0 allows remote attackers to bypass authentication and gain administrative access via a userid=1&lvl=1 value for the twLTadmin cookie.	2009-05-12	7.5	CVE-1617 BID MILV SECU
teraway -- livehelp	Teraway LiveHelp 2.0 allows remote attackers to bypass authentication and gain administrative access via a pwd=&lvl=1&usr=&alias=admin&userid=1 value for the TWLHadmin cookie.	2009-05-12	7.5	CVE-1618 BID MILV SECU
teraway -- filestream	Teraway FileStream 1.0 allows remote attackers to bypass authentication and gain administrative access by setting the twFSadmin cookie to 1.	2009-05-12	7.5	CVE-1619 BID MILV SECU
tribiq -- tribiq_cms	** DISPUTED ** Tribiq CMS 5.0.9a beta allows remote attackers to bypass authentication and gain administrative access by setting the COOKIE_LAST_ADMIN_USER and COOKIE_LAST_ADMIN_LANG cookies. NOTE: a third party reports that the vendor disputes the existence of this issue.	2009-05-11	7.5	CVE-6804 XF BID MILV
	Heap-based buffer overflow in popcorn.exe in Ultrafunk Popcorn 1.87 allows remote			CVE-1617

ultrafunk -- popcorn	POP3 servers to cause a denial of service (application crash) via a long string in a +OK response. NOTE: some of these details are obtained from third party information.	2009-05-15	9.3	104/ VUPI BID MILA
will_kraft -- ez-blog	SQL injection vulnerability in public/specific.php in EZ-Blog before Beta 2 20090427, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the category parameter.	2009-05-12	7.5	CVE-1626 BID MILA CON.
yigit_aybuga -- dizi_portali	SQL injection vulnerability in diziler.asp in Yigit Aybuga Dizi Portali allows remote attackers to execute arbitrary SQL commands via the id parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-05-11	7.5	CVE-6803 XF BID

[Back to top](#)

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
7-shop -- 7shop	Unrestricted file upload vulnerability in includes/imageupload.php in 7Shop 1.1 and earlier allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in images/artikel/.	2009-05-12	6.8	CVE-2008-6806 XF VUPEN BID MILWoRM
a-a-s_application_access_server -- a-a-s_application_access_server	Multiple cross-site request forgery (CSRF) vulnerabilities in index.aas in Application Access Server (A-A-S) 2.0.48 allow remote attackers to hijack the authentication of administrators for requests that (1) execute arbitrary programs via a command job, (2) stop services via a setservice job, or (3) terminate processes via a killprocess job.	2009-05-14	6.8	CVE-2009-1464 MISC MISC BID BUGTRAQ SECTRACK SECUNIA
antony_lesuisse -- ajaxterm	ajaxterm.js in AjaxTerm 0.10 and earlier generates session IDs with predictable random numbers based on certain JavaScript functions, which makes it easier for remote attackers to (1) hijack a session or (2) cause a denial of service (session ID exhaustion) via a brute-force attack.	2009-05-14	6.8	CVE-2009-1629 XF BUGTRAQ MLIST MISC
apple -- mac_os_x apple -- mac_os_x apple -- mac_os_x_server	CFNetwork in Apple Mac OS X 10.5 before 10.5.7 does not properly parse noncompliant Set-Cookie headers, which allows remote attackers to obtain sensitive information by sniffing the network for "secure cookies" that are sent over unencrypted HTTP connections.	2009-05-13	4.3	CVE-2009-0144 CONFIRM APPLE
apple -- mac_os_x apple -- mac_os_x_server	CoreGraphics in Apple Mac OS X 10.4.11 and 10.5 before 10.5.7 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted PDF file that triggers memory corruption.	2009-05-13	6.8	CVE-2009-0145 CONFIRM APPLE
apple -- mac_os_x apple -- mac_os_x_server	Stack-based buffer overflow in Apple Mac OS X 10.5 before 10.5.7 allows local users to gain privileges or cause a denial of service (application crash) by attempting to mount a crafted sparse disk image.	2009-05-13	4.6	CVE-2009-0150 CONFIRM APPLE

apple -- mac_os_x apple -- mac_os_x_server	iChat in Apple Mac OS X 10.5 before 10.5.7 disables SSL for AOL Instant Messenger (AIM) communication in certain circumstances that are inconsistent with the Require SSL setting, which allows remote attackers to obtain sensitive information by sniffing the network.	2009-05-13	5.0	<a href="#">CVE-2009-0152</a> CONFIRM APPLE
apple -- mac_os_x apple -- mac_os_x_server	International Components for Unicode (ICU) in Apple Mac OS X 10.5 before 10.5.7 does not properly handle invalid byte sequences during Unicode conversion, which might allow remote attackers to conduct cross-site scripting (XSS) attacks.	2009-05-13	4.3	<a href="#">CVE-2009-0153</a> CONFIRM APPLE
apple -- mac_os_x apple -- mac_os_x_server	Heap-based buffer overflow in Apple Type Services (ATS) in Apple Mac OS X 10.4.11 and 10.5 before 10.5.7 allows remote attackers to execute arbitrary code via a crafted Compact Font Format (CFF) font.	2009-05-13	6.8	<a href="#">CVE-2009-0154</a> CONFIRM APPLE
apple -- mac_os_x apple -- mac_os_x_server	Integer underflow in CoreGraphics in Apple Mac OS X 10.5 before 10.5.7 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted PDF file that triggers a heap-based buffer overflow.	2009-05-13	6.8	<a href="#">CVE-2009-0155</a> CONFIRM APPLE
apple -- mac_os_x apple -- mac_os_x_server	Launch Services in Apple Mac OS X 10.4.11 and 10.5 before 10.5.7 allows remote attackers to cause a denial of service (persistent Finder crash) via a crafted Mach-O executable that triggers an out-of-bounds memory read.	2009-05-13	4.3	<a href="#">CVE-2009-0156</a> CONFIRM APPLE
apple -- mac_os_x apple -- mac_os_x_server	Heap-based buffer overflow in CFNetwork in Apple Mac OS X 10.5 before 10.5.7 allows remote web servers to execute arbitrary code or cause a denial of service (application crash) via long HTTP headers.	2009-05-13	6.8	<a href="#">CVE-2009-0157</a> CONFIRM APPLE
apple -- mac_os_x apple -- mac_os_x_server	Stack-based buffer overflow in telnet in Apple Mac OS X 10.4.11 and 10.5 before 10.5.7 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a long hostname for a telnet server.	2009-05-13	6.8	<a href="#">CVE-2009-0158</a> CONFIRM APPLE
apple -- mac_os_x apple -- mac_os_x_server	QuickDraw Manager in Apple Mac OS X 10.4.11 and 10.5 before 10.5.7 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted PICT image that triggers memory corruption.	2009-05-13	6.8	<a href="#">CVE-2009-0160</a> CONFIRM APPLE
apple -- mac_os_x apple -- mac_os_x_server	The OpenSSL::OCSP module for Ruby in Apple Mac OS X 10.5 before 10.5.7 misinterprets an unspecified invalid response as a successful OCSP certificate validation, which might allow remote attackers to spoof certificate authentication via a revoked certificate.	2009-05-13	6.4	<a href="#">CVE-2009-0161</a> CONFIRM APPLE
apple -- safari	Cross-site scripting (XSS) vulnerability in Safari before 3.2.3, and 4 Public Beta, on Apple Mac OS X 10.5 before 10.5.7 and Windows allows remote attackers to inject arbitrary web script or HTML via a crafted feed: URL.	2009-05-13	4.3	<a href="#">CVE-2009-0162</a> CONFIRM APPLE APPLE APPLE
apple -- mac_os_x apple -- mac_os_x_server	Help Viewer in Apple Mac OS X 10.4.11 and 10.5 before 10.5.7 does not verify that certain Cascading Style Sheets (CSS) are located in a registered help book, which allows remote attackers to execute arbitrary code via a help: URL that triggers invocation of AppleScript files.	2009-05-13	6.8	<a href="#">CVE-2009-0942</a> CONFIRM APPLE
	Help Viewer in Apple Mac OS X 10.4.11 and 10.5 before			<a href="#">CVE-2009-</a>

apple -- mac_os_x apple -- mac_os_x_server	10.5.7 does not verify that HTML pathnames are located in a registered help book, which allows remote attackers to execute arbitrary code via a help: URL that triggers invocation of AppleScript files.	2009-05-13	6.8	CVE-2009-0943 CONFIRM APPLE
apple -- mac_os_x apple -- mac_os_x_server	The Microsoft Office Spotlight Importer in Spotlight in Apple Mac OS X 10.4.11 and 10.5 before 10.5.7 does not properly validate Microsoft Office files, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a file that triggers memory corruption.	2009-05-13	6.8	CVE-2009-0944 CONFIRM APPLE
battleblog -- battle_blog	Unrestricted file upload vulnerability in admin/uploadform.asp in Battle Blog 1.25 allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file.	2009-05-11	6.8	CVE-2009-1609 XF BID MILWoRM SECUNIA
branden_robinson -- xvfb-run debian -- debian_linux redhat -- fedora ubuntu -- linux	xvfb-run 1.6.1 in Debian GNU/Linux, Ubuntu, Fedora 10, and possibly other operating systems place the magic cookie (MCOOKIE) on the command line, which allows local users to gain privileges by listing the process and its arguments.	2009-05-06	4.6	CVE-2009-1573 XF BID MLIST MLIST CONFIRM
cgi_rescue -- cgi_rescue_minibbs	Cross-site scripting (XSS) vulnerability in CGI RESCUE MiniBBS 8t before 8.95t, 8 before 8.95, 9 before 9.08, and 10 before 10.32 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-05-08	4.3	CVE-2009-1588 JVND JVN
cgi_rescue -- cgi_rescue_minibbs22	Unspecified vulnerability in CGI RESCUE MiniBBS22 before 1.01 allows remote attackers to send email to arbitrary recipients via unknown vectors.	2009-05-08	5.0	CVE-2009-1589 CONFIRM JVND JVN
cgi_rescue -- form2mail	Unspecified vulnerability in CGI RESCUE FORM2MAIL before 1.42 allows remote attackers to send email to arbitrary recipients via a web form.	2009-05-08	5.0	CVE-2009-1590 OSVDB JVN
cgi_rescue -- cgi_web_mailer	CRLF injection vulnerability in CGI RESCUE Web Mailer before 1.04 allows remote attackers to inject arbitrary HTTP headers, and conduct cross-site scripting (XSS) or HTTP response splitting attacks, via CRLF sequences in an unspecified web form.	2009-05-08	4.3	CVE-2009-1591 CONFIRM JVN
cisco -- wvc54gca	The Cisco Linksys WVC54GCA wireless video camera with firmware 1.00R22 and 1.00R24 sends configuration data in response to a Setup Wizard remote-management command, which allows remote attackers to obtain sensitive information such as passwords by reading the SetupWizard.exe process memory, a related issue to CVE-2008-4390.	2009-05-06	5.0	CVE-2009-1555 VUPEN MISC SECUNIA
coppermine -- coppermine_photo_gallery	Cross-site scripting (XSS) vulnerability in docs/showdoc.php in Coppermine Photo Gallery (CPG) before 1.4.22 allows remote attackers to inject arbitrary web script or HTML via the css parameter, a different vector than CVE-2008-0505.	2009-05-11	4.3	CVE-2009-1616 CONFIRM
davlin -- thickbox_gallery	Directory traversal vulnerability in index.php in Thickbox Gallery 2 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the	2009-05-12	6.8	CVE-2009-1625 BID MILWoRM

	In parameter.			MILWoRM SECUNIA
dew-code -- dew-newphplinks	Cross-site scripting (XSS) vulnerability in index.php in Dew-NewPHPLinks 2.0 allows remote attackers to inject arbitrary web script or HTML via the PID parameter.	2009-05-12	4.3	CVE-2009-1623 BID MILWoRM
dew-code -- dew-newphplinks	Directory traversal vulnerability in index.php in Dew-NewPHPLinks 2.0 allows remote attackers to read arbitrary files via a .. (dot dot) in the show parameter.	2009-05-12	5.0	CVE-2009-1624 BID MILWoRM
google -- chrome	Multiple integer overflows in Skia, as used in Google Chrome 1.x before 1.0.154.64 and 2.x, and possibly Android, might allow remote attackers to execute arbitrary code in the renderer process via a crafted (1) image or (2) canvas.	2009-05-07	6.8	CVE-2009-1442 CONFIRM
gowondesigns -- leap	Multiple SQL injection vulnerabilities in leap.php in Leap CMS 0.1.4, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) searchterm or (2) email parameter.	2009-05-11	6.8	CVE-2009-1613 MILWoRM MILWoRM SECUNIA
gowondesigns -- leap	Unrestricted file upload vulnerability in Leap CMS 0.1.4 allows remote attackers to execute arbitrary code by uploading a file with an executable extension via an admin.system.files (aka Manage Files) request to the default URI, then accessing the file via a direct request.	2009-05-11	6.8	CVE-2009-1615 MILWoRM
icewarp -- email_server icewarp -- webmail_server	Multiple cross-site scripting (XSS) vulnerabilities in IceWarp eMail Server and WebMail Server before 9.4.2 allow remote attackers to inject arbitrary web script or HTML via (1) the body of a message, related to the email view and incorrect HTML filtering in the cleanHTML function in server/inc/tools.php; or the (2) title, (3) link, or (4) description element in an RSS feed, related to the getHTML function in server/inc/rss/item.php.	2009-05-05	4.3	CVE-2009-1467 MISC
icewarp -- email_server icewarp -- webmail_server	Multiple SQL injection vulnerabilities in the search form in server/webmail.php in the Groupware component in IceWarp eMail Server and WebMail Server before 9.4.2 allow remote authenticated users to execute arbitrary SQL commands via the (1) sql and (2) order_by elements in an XML search query.	2009-05-05	6.5	CVE-2009-1468 SECTRACK BID BUGTRAQ MISC OSVDB
icewarp -- email_server icewarp -- webmail_server	CRLF injection vulnerability in the Forgot Password implementation in server/webmail.php in IceWarp eMail Server and WebMail Server before 9.4.2 makes it easier for remote attackers to trick a user into disclosing credentials via CRLF sequences preceding a Reply-To header in the subject element of an XML document, as demonstrated by triggering an e-mail message from the server that contains a user's correct credentials, and requests that the user compose a reply that includes this message.	2009-05-05	4.3	CVE-2009-1469 XF SECTRACK BID BUGTRAQ MISC OSVDB
igniterealtime -- openfire	The jabber:iq:auth implementation in IQAuthHandler.java in Ignite Realtime Openfire before 3.6.4 allows remote authenticated users to change the passwords of arbitrary accounts via a modified username element in a passwd_change action.	2009-05-11	4.0	CVE-2009-1595 VUPEN BID CONFIRM CONFIRM

				CONFIRM
igniterealtime -- openfire	Ignite Realtime Openfire before 3.6.5 does not properly implement the register.password (aka canChangePassword) console configuration setting, which allows remote authenticated users to bypass intended policy and change their own passwords via a passwd_change IQ packet.	2009-05-11	4.0	CVE-2009-1596 BID CONFIRM CONFIRM
ipsec-tools -- ipsec-tools	racoon/isakmp_frag.c in ipsec-tools before 0.7.2 allows remote attackers to cause a denial of service (crash) via crafted fragmented packets without a payload, which triggers a NULL pointer dereference.	2009-05-06	5.0	CVE-2009-1574 CONFIRM MLIST MLIST
ipsec-tools -- ipsec-tools	Multiple memory leaks in Ipsec-tools before 0.7.2 allow remote attackers to cause a denial of service (memory consumption) via vectors involving (1) signature verification during user authentication with X.509 certificates, related to the eay_check_x509sign function in src/racoon/crypto_openssl.c; and (2) the NAT-Traversal (aka NAT-T) keepalive implementation, related to src/racoon/natTraversal.c.	2009-05-14	5.0	CVE-2009-1632 MLIST
klinzmann -- a-a-s	Application Access Server (A-A-S) 2.0.48 stores (1) passwords and (2) the port keyword in cleartext in aas.ini, which allows local users to obtain sensitive information by reading this file.	2009-05-14	5.0	CVE-2009-1466 MISC BID BUGTRAQ SECTRACK
linkbase -- linkbase	Cross-site scripting (XSS) vulnerability in the administrator panel in phpForm.net LinkBase 2.0 allows remote attackers to inject arbitrary web script or HTML via the username in a registration, which is not properly handled when the administrator accesses the Users menu.	2009-05-11	4.3	CVE-2009-1607 XF BID MILWoRM
linux -- kernel	The nfs_permission function in fs/nfs/dir.c in the NFS client implementation in the Linux kernel 2.6.29.3 and earlier, when atomic_open is available, does not check execute (aka EXEC or MAY_EXEC) permission bits, which allows local users to bypass permissions and execute files, as demonstrated by files on an NFSv4 fileserver.	2009-05-14	4.4	CVE-2009-1630 MLIST CONFIRM
mata -- matachat	Multiple cross-site scripting (XSS) vulnerabilities in input.php in MataChat allow remote attackers to inject arbitrary web script or HTML via the (1) nickname and (2) color parameters.	2009-05-12	4.3	CVE-2009-1620 BID BUGTRAQ
micgr -- mic_blog	Multiple SQL injection vulnerabilities in Mic_Blog 0.0.3, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) cat parameter to category.php, the (2) user parameter to login.php, and the (3) site parameter to register.php.	2009-05-11	6.8	CVE-2008-6805 BID OSVDB OSVDB OSVDB MILWoRM SECUNIA
mortbay -- jetty	Cross-site scripting (XSS) vulnerability in Mort Bay Jetty before 6.1.17 allows remote attackers to inject arbitrary web script or HTML via a directory listing request containing a ; (semicolon) character.	2009-05-05	4.3	CVE-2009-1524 CONFIRM
				CVE-2009-

nucleustechnologies -- kernel_recovery	Stack-based buffer overflow in Nucleus Data Recovery Kernel Recovery for Novell 4.03 allows user-assisted attackers to execute arbitrary code via a crafted .NKNT file.	2009-05-15	6.8	1639 BID MISC MISC SECUNIA
opencart -- opencart	Directory traversal vulnerability in index.php in OpenCart 1.1.8 allows remote attackers to read arbitrary files via a .. (dot dot) in the route parameter.	2009-05-12	5.0	CVE-2009-1621 BID MILWoRM SECUNIA
opense-project -- opense	src/tools/pkcs11-tool.c in pkcs11-tool in OpenSC 0.11.7, when used with unspecified third-party PKCS#11 modules, generates RSA keys with incorrect public exponents, which allows attackers to read the cleartext form of messages that were intended to be encrypted.	2009-05-11	4.3	CVE-2009-1603 MLIST
pablosoftwaresolutions -- quick'n_easy_mail_server	Pablo Software Solutions Quick 'n Easy Mail Server 3.3 allows remote attackers to cause a denial of service (daemon outage or CPU consumption) via multiple long SMTP commands, as demonstrated by HELO commands.	2009-05-11	5.0	CVE-2009-1602 XF BID MILWoRM SECUNIA OSVDB
pango -- pango	Integer overflow in the pango_glyph_string_set_size function in pango/glyphstring.c in Pango before 1.24 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long glyph string that triggers a heap-based buffer overflow, as demonstrated by a long document.location value in Firefox.	2009-05-11	6.8	CVE-2009-1194 MISC
quagga -- quagga_routing_software_suite	The BGP daemon (bgpd) in Quagga 0.99.11 and earlier allows remote attackers to cause a denial of service (crash) via an AS path containing ASN elements whose string representation is longer than expected, which triggers an assert error.	2009-05-06	5.0	CVE-2009-1572 DEBIAN MLIST CONFIRM
ro20 -- tematres	Multiple SQL injection vulnerabilities in TemaTres 1.0.3 and 1.031, when magic_quotes_gpc is disabled, allow remote attackers or remote authenticated users to execute arbitrary SQL commands via the (1) mail, (2) password, and (3) letra parameters to index.php; (4) y and (5) m parameters to sobre.php; and the (6) dcTema, (7) madsTema, (8) zthesTema, (9) skosTema, and (10) xtmTema parameters to xml.php.	2009-05-07	6.0	CVE-2009-1584 BID BUGTRAQ BUGTRAQ MILWoRM MILWoRM SECUNIA OSVDB OSVDB
ro20 -- tematres	Multiple SQL injection vulnerabilities in TemaTres 1.031, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) id_correo_electronico and (2) id_password parameters to login.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-05-07	4.4	CVE-2009-1585 SECUNIA OSVDB
sendmail -- sendmail	Heap-based buffer overflow in Sendmail before 8.13.2 allows remote attackers to cause a denial of service (daemon crash) and possibly execute arbitrary code via a long X- header, as demonstrated by an X-Testing header.	2009-05-05	5.0	CVE-2009-1490 CONFIRM
				CVE-2009-

simplecustomer -- simple_customer	profile.php in Simple Customer 1.3 does not require administrative authentication, which allows remote attackers to change the admin e-mail address and password via the email and password parameters.	2009-05-15	6.4	1637 XF BID MILWoRM SECUNIA OSVDB
squirrelmail -- squirrelmail	Multiple cross-site scripting (XSS) vulnerabilities in SquirrelMail before 1.4.18 allow remote attackers to inject arbitrary web script or HTML via vectors involving (1) certain encrypted strings in e-mail headers, related to contrib/decrypt_headers.php; (2) PHP_SELF; and (3) the query string (aka QUERY_STRING).	2009-05-14	4.3	CVE-2009-1578 FEDORA FEDORA XF VUPEN CONFIRM CONFIRM BID MANDRIVA CONFIRM CONFIRM CONFIRM CONFIRM
squirrelmail -- squirrelmail	The map_yp_alias function in functions/imap_general.php in SquirrelMail before 1.4.18 allows remote attackers to execute arbitrary commands via shell metacharacters in a username string that is used by the ypmatch program.	2009-05-14	6.8	CVE-2009-1579 FEDORA FEDORA VUPEN CONFIRM BID MANDRIVA CONFIRM CONFIRM
squirrelmail -- squirrelmail	functions/mime.php in SquirrelMail before 1.4.18 does not protect the application's content from Cascading Style Sheets (CSS) positioning in HTML e-mail messages, which allows remote attackers to spoof the user interface, and conduct cross-site scripting (XSS) and phishing attacks, via a crafted message.	2009-05-14	4.3	CVE-2009-1581 CONFIRM
sun -- glassfish_enterprise_server	Multiple cross-site scripting (XSS) vulnerabilities in the Admin Console in Sun GlassFish Enterprise Server 2.1 allow remote attackers to inject arbitrary web script or HTML via the query string to (1) applications/applications.jsf, (2) configuration/configuration.jsf, (3) customMBeans/customMBeans.jsf, (4) resourceNode/resources.jsf, (5) sysnet/registration.jsf, or (6) webService/webServicesGeneral.jsf; or the name parameter to (7) configuration/auditModuleEdit.jsf, (8) configuration/httpListenerEdit.jsf, or (9) resourceNode/jdbcResourceEdit.jsf.	2009-05-06	4.3	CVE-2009-1553 MLIST MLIST MLIST
sun -- woodstock	Cross-site scripting (XSS) vulnerability in ThemeServlet.java in Sun Woodstock 4.2, as used in Sun GlassFish Enterprise Server and other products, allows remote attackers to inject arbitrary web script or HTML via a UTF-7 string in the PATH_INFO, which is displayed on the 404 error page, as demonstrated by the PATH_INFO to theme/META-INF.	2009-05-06	4.3	CVE-2009-1554 MLIST
	The Ubuntu clamav-milter.init script in clamav-milter			

ubuntu -- linux	before 0.95.1+dfsg-1ubuntu1.2 in Ubuntu 9.04 sets the ownership of the current working directory to the clamav account, which might allow local users to bypass intended access restrictions via read or write operations involving this directory.	2009-05-11	6.8	<a href="#">CVE-2009-1601</a> <a href="#">XF</a> <a href="#">BID</a>
-----------------	---	------------	-----	--

[Back to top](#)

#### Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gnome -- evolution	The Mailer component in Evolution 2.26.1 and earlier uses world-readable permissions for the .evolution directory, and certain directories and files under .evolution/ related to local mail, which allows local users to obtain sensitive information by reading these files.	2009-05-14	2.1	<a href="#">CVE-2009-1631</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
gowondesigns -- leap	Multiple cross-site scripting (XSS) vulnerabilities in Leap CMS 0.1.4 allow remote attackers to inject arbitrary web script or HTML via (1) the msg parameter (aka the message in an article comment) or (2) the searchterm parameter (aka the search post form). NOTE: some of these details are obtained from third party information.	2009-05-11	2.6	<a href="#">CVE-2009-1614</a> <a href="#">MILWoRM</a> <a href="#">SECUNIA</a>

[Back to top](#)

Last updated May 18, 2009



[Print This Document](#)